



UNITED STATES PATENT AND TRADEMARK OFFICE

mm

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/765,932 | 01/29/2004 | Goran Ekstrom | 003301-114 | 1870 |

21839 7590 06/08/2007
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER

SANDOVAL, KRISTIN D

ART UNIT PAPER NUMBER

2132

MAIL DATE DELIVERY MODE

06/08/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/765,932

Applicant(s)

EKSTROM, GORAN

Examiner

Kristin D. Sandoval

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 January 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- *.See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>6/5/07</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-32 are pending.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: It seems that although each item is assigned a reference numeral none of the items contain any text despite the specification referencing the numerals in association with certain aspects of the invention. For example, pg. 16 of applicant's specification states, "In an extracting step 100, the encrypted encryption key K1, which was sent with the consignment, is extracted (lines 29-31)". However, item 100 of figure 4 is not labeled an extracting step. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Art Unit: 2132

3. Claims 1-32 objected to because of the following informalities: In claims 2, 15 and 23 the “encryption key” and “supplementary encryption key” in claims 1, 14 and 22 are renamed as “first encryption key” and “second encryption key”. It is confusing to have two names used to describe the same thing especially for two different items. It is requested that a single name for each encryption key is used in order to simplify interpretation of the claims. Appropriate correction is required.

4. Claims 2, 15 and 23 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claims 1, 14 and 22 already state the limitation, “said encryption key, upon positive identification of the receiver, and enabling, with the involvement of a supplementary encryption key of the receiver, decryption of the package of information.” Claims 2, 15 and 23 do not further limit these claims since a key from the receiver and a key from the third party are needed in order to decrypt the package of information.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 3, 24, 31 and 32 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2132

With regard to claims 3 and 24 a dependent claim must refer to limitations occurring in the claims it depends from directly and not 2 or 3 removed. The step of “encrypting said package of information” is stated in claim 1, not in the claim that claim 3 depends on directly which is claim 2.

With regard to claims 31 and 32, these claims depend upon claim 1 which is a method claim. Any depending claims cannot change the statutory category to which they belong, they must all be method claims, thus the system claim of claim 31 and the product claim of claim 32 must be method claims to depend upon claim 1.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-3, 5-24 and 26-32 rejected under 35 U.S.C. 102(e) as being anticipated by Andivahis et al. (Andivahis), U.S. Patent No. 7,146,009.

As per claims 1, 2, 14, 15, 22, 23, 31 and 32:

Andivahis discloses a method of enabling secure transfer of a package of information in a digital communications network from a sender to a receiver, comprising the steps of:

encrypting said package of information (5:60-6:11);

providing said encrypted package of information to the receiver (6:12-16); and

Art Unit: 2132

providing to a third party an encryption key having such a format that it is unable to decrypt said package of information, said encryption key, upon positive identification of the receiver, being providable from said third party to the receiver, and enabling, with the involvement of a supplementary encryption key of the receiver, decryption of the package of information (7:1-6).

As per claims 3 and 24:

Andivahis discloses a method in which encrypting the package of information comprises the steps of:

combining said first and second encryption keys for generating a combined encryption key (9:45-62); and encrypting said package of information by means of said generated combined encryption key (9:45-62).

As per claim 5:

Andivahis discloses a method in which the information is encrypted by a main encryption key, said main encryption key then being divided into said first encryption key which is provided to the receiver and said second encryption key which is provided to the third party (5:13-30).

As per claims 6 and 26:

Andivahis discloses a method in which the step of providing a first encryption key to the receiver is preceded by the step of encrypting said first encryption key with a public key of the receiver (9:55-62), wherein the receiver is able to decrypt said encrypted first encryption key with a private key (10:39-47).

As per claims 7, 8, 16, 17, 27 and 28

Andivahis discloses a method in which the step of providing to a third party an encryption key is preceded by the steps of:

encrypting said package of information with that encryption key (5:60-6:11); and encrypting that encryption key with a public key of the receiver (5:13-21), wherein said encrypted encryption key is decryptable by said supplementary encryption key which is a private key of the receiver so as to enable decryption of the package of information (7:1-6).

As per claims 9, 10 and 18:

Andivahis discloses a method in which instructions are sent to the third party, said instructions defining under what conditions the encryption key provided to the third party may be retrieved by the receiver of the package of information (11:11-25).

As per claims 11, 12, 19, 20, 29:

Andivahis discloses a method in which the secure transfer of said package of information is only completely performed if the receiver and the sender are identified by means of a registered certificate (4:40-45, 6:24-29, 13:14-20, 16:7-23).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 4 and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over Andihavis as applied to claims 1, 14 and 22 above and further in view of Luo, U.S. Patent No. 5,909,491.

Art Unit: 2132

As per claims 4 and 25:

Andivahis fails to teach the message being encrypted by one encryption key, then encrypted again with another encryption key. However, Luo discloses a method wherein a message is encrypted by a sending transceiver and encrypted again by a receiving transceiver then the doubly encrypted message is sent back to the sending transceiver (abstract). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to encrypt combine the invention of Luo with the invention of Andivahis because this way a particular user's decryption key is known only at the transceiving device of the particular user and the device need only use that particular user's encryption/decryption algorithms and encryption key as taught by Luo (4:58-65).

8. Claims 13, 21 and 30 rejected under 35 U.S.C. 103(a) as being unpatentable over Andihavis as applied to claims 1, 14 and 22 above and further in view of Fielder et al. (Fielder), U.S. Patent No. 6,049,612.

As per claim 13, 21 and 30:

Andivahis teaches a method further comprising the steps of:

obtaining from the third party a first hash value which has been derived from the contents of said package of information by means of a hash function (12:11-28). Andivahis fails to teach calculating a second hash value and comparing the first and second hash values in order to detect if the message has been tampered with. However, Fielder discloses utilizing a hash to calculate a message integrity code for a given message and recalculating the message integrity code and comparing the two values to detect whether the message was tampered with (5:37-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

Art Unit: 2132

recalculate the hash value and compare them in order to ensure the message wasn't tampered with in order to ensure the message is not altered in any way as taught by Fielder (4:40-45).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin D. Sandoval whose telephone number is 571-272-7958.

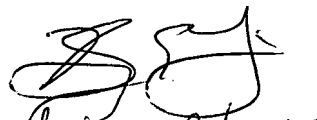
The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristin D Sandoval
Examiner
Art Unit 2132

1005
KDS


Benjamin E. Lerner
Examiner Art 2132